On the Diameter of Matroid Ports*

Jaume Martí-Farré, Carles Padró and Leonor Vázquez†

Dept. de Matemàtica Aplicada IV, Universitat Politècnica de Catalunya
C. Jordi Girona, 1–3, mòdul C5, Campus Nord, 08034 Barcelona, Spain
{jaumem,cpadro,leonor}@ma4.upc.edu

Submitted: May 21, 2008; Accepted: Jul 2, 2008; Published: Jul 14, 2008
Mathematics Subject Classifications: 94A62, 52B40

Abstract

A clutter or antichain on a set defines a hypergraph. Matroid ports are a special class of clutters, and this paper deals with the diameter of matroid ports, that is, the diameter of the corresponding hypergraphs. Specifically, we prove that the diameter of every matroid port is at most 2. The main interest of our result is its application to secret sharing. Brickell and Davenport proved in 1989 that the minimal qualified subsets of every ideal secret sharing scheme form a matroid port. Therefore, our result provides a new necessary condition for an access structure to admit an ideal secret sharing scheme.

Keywords: Matroids, Matroid ports, Secret sharing, Ideal secret sharing schemes.

1 Introduction

A *clutter* or *antichain* on a set P is a family Λ of subsets of P such that $A \not\subseteq B$ for every pair of different elements $A, B \in \Lambda$. For instance, the circuits of a matroid form a clutter on the ground set. Given a matroid $\mathcal{M}$ and a point $p_0 \in Q$ in the ground set, the *port of the matroid* $\mathcal{M}$ *at the point* p_0 is the clutter $\mathcal{M}_{p_0}$ on the set $P = Q - \{p_0\}$ defined by

$$\mathcal{M}_{p_0} = \{A \subseteq P \,:\, A \cup \{p_0\} \text{ is a circuit of } \mathcal{M}\}.$$

Matroid ports were introduced in 1964 by Lehman [6] to solve the Shannon switching game. By extending a previous characterization by Lehman [7], Seymour [11] gave in 1976 several characterizations of matroid ports, one of them in terms of forbidden minors.

Every clutter Λ on a set P defines a hypergraph whose vertices are the elements of P while its hyperedges are the sets in Λ. The diameter of a clutter is defined in the following

*This work was partially supported by the Spanish Ministry of Education and Science under project TSI2006-02731.

†This work was partially supported under CONACYT grant 173985.

as the diameter of the corresponding hypergraph. For a clutter Λ on a set P and two points $p_1, p_2 \in P$, a *path* Π_{p_1,p_2} of *length* r between the points p_1 and p_2 in the clutter Λ is a sequence $\Pi_{p_1,p_2} = (A_1, \ldots, A_r)$ of sets in Λ such that $p_1 \in A_1$, $p_2 \in A_r$, and $A_i \cap A_{i+1} \neq \emptyset$ if $1 \leq i \leq r-1$. A clutter is said to be *path-connected* if there is a path between every pair of vertices. The minimum length of all paths between p_1 and p_2 is called the *distance* between these two points, and it is denoted by $d_\Lambda(p_1, p_2)$. The *diameter* of a clutter is the maximum distance between all pairs of vertices. In this paper, we prove the following property of matroid ports.

Theorem 1. *The diameter of every path-connected matroid port is at most* 2.

Since there exist efficient algorithms to compute the diameter of a hypergraph, this result provides a necessary condition for a clutter to be a matroid port that can be efficiently checked. The main application of our result is in secret sharing, specifically, in the characterization of the access structures of ideal secret sharing schemes. As a consequence of the results by Brickell and Davenport [4], for every ideal secret sharing scheme, the clutter formed by its minimal qualified subsets is a matroid port. Therefore, our result provides an easily checkable necessary condition for an access structure to admit an ideal secret sharing scheme.

Some basic facts about secret sharing and its connection to matroid ports are presented in Section 2. Theorem 1 is proved in Section 3, while some extensions of this result and its application to secret sharing are discussed in Section 4.

2 Secret Sharing and Matroid Ports

The main definitions and terminology, and some basic facts about matroid ports are recalled in this section. In addition, we discuss the connections of matroids ports to secret sharing. The reader is referred to the book by Oxley [9] for the concepts from matroid theory that are not defined here and to [15] for a survey on secret sharing.

Matroids are combinatorial objects that generalize the properties of linear dependence among a finite set of vectors. There are many different equivalent definitions of matroid. The one we present here is based on the axioms of the circuits, the minimal dependent sets. A *matroid* $\mathcal{M}$ is a pair $\mathcal{M} = (Q, \mathcal{C})$ where Q is a finite set, the *ground set* of $\mathcal{M}$, and $\mathcal{C}$ is a clutter on Q such that

1. $\emptyset \notin \mathcal{C}$, and
2. if C_1 and C_2 are different elements in $\mathcal{C}$ and $p \in C_1 \cap C_2$, then there exists $C_3 \in \mathcal{C}$ such that $C_3 \subseteq (C_1 \cup C_2) - \{p\}$.

The subsets in $\mathcal{C}$ are the *circuits* of the matroid. A matroid is said to be *connected* if every two points lie in a common circuit. A clutter Λ on a set P is said to be *connected* if $P = \bigcup_{A \in \Lambda} A$. From [9, Proposition 4.1.2], a matroid $\mathcal{M}$ is connected if and only if any of its ports $\mathcal{M}_{p_0}$ is a connected clutter, and in this case all ports of $\mathcal{M}$ are connected.

Lehman [6] proved that a connected matroid can be determined from any of its ports. Since it will be used later, we describe in detail this result. A proof for it can be found in [9, Theorem 4.3.2]. For a clutter Λ on a set P and a subset $X \subseteq P$, consider $\Lambda(X) = \{A \subseteq X : A \in \Lambda\}$, the *induced clutter of* Λ *on* X. Consider as well the sets $I(X)$ and $E(X)$ defined by $I(X) = \bigcap\{A : A \in \Lambda(X)\}$ and $E(X) = X - I(X)$. Let $\mathcal{C}_2(\Lambda) = \min \mathcal{C}_2^+(\Lambda)$ be the clutter on P formed by the minimal subsets of

$$\mathcal{C}_2^+(\Lambda) = \{E(A_1 \cup A_2) : A_1, A_2 \in \Lambda, \ A_1 \neq A_2\}.$$

Finally, on the set $Q = P \cup \{p_0\}$ where $p_0 \notin P$, consider the clutter $\mathcal{C}_1(\Lambda) = \{A \cup \{p_0\} : A \in \Lambda\}$ and let $\mathcal{C}(\Lambda) = \mathcal{C}_1(\Lambda) \cup \mathcal{C}_2(\Lambda)$. Now, by using these notations, the result by Lehman can be stated as follows.

Theorem 2. *Let Λ be a connected clutter on a set P and $Q = P \cup \{p_0\}$, where $p_0 \notin P$. Then the clutter Λ is a matroid port on P if and only if $\mathcal{M} = (Q, \mathcal{C}(\Lambda))$ is a matroid with ground set Q, and in this case $\mathcal{M}$ is the only matroid with $\Lambda = \mathcal{M}_{p_0}$.*

This result provides a characterization of matroid ports. Other characterizations were given later on by Lehman [7] and Seymour [11]. By combining the results by Seymour [11] with some results and techniques from secret sharing, a new characterization of matroid ports has been found recently [8]. This characterization, which is stated in Theorem 3, is the one that we will use subsequently in this paper.

Secret sharing, which was independently introduced by Blakley [1] and Shamir [13] in 1979, is an important primitive in cryptography that is used as a building-block in many different cryptographic protocols. A *secret sharing scheme* is a method of distributing shares of a secret value among a *set of participants* P in such a way that only certain specified subsets of participants, the *qualified subsets*, can reconstruct the secret value by pooling their shares, while the shares of the participants in a *non-qualified subset* provide absolutely no information about the value of the secret. The *access structure* Γ is the collection of the qualified subsets. Since every subset containing a qualified subset must be qualified, the access structure is a monotone increasing family of subsets, which is determined by the clutter $\min \Gamma$ of its minimal elements.

The complexity of a secret sharing scheme is usually measured by the length of the shares. The *information rate* $\rho(\Sigma)$ of a secret sharing scheme Σ is defined as the ratio between the length (in bits) of the secret and the maximum length of the shares given to the participants. A secret sharing scheme is said to be *ideal* if every share has the same length as the secret, which is the best possible situation. Not every access structure admits an ideal scheme. The characterization of the *ideal access structures*, that is, the access structures of ideal secret sharing schemes, is a difficult, long-standing open problem. Brickell and Davenport [4] proved in 1991 that, for every ideal access structure Γ, the clutter $\min \Gamma$ is a matroid port. Seymour [12] proved that this necessary condition for an access structure to be ideal is not sufficient. Specifically, he proved that the access structures induced by the ports of the Vamos matroid are not ideal. As a consequence of the results by Brickell [3], the ports of linearly representable matroids define ideal access structures. This sufficient condition is not necessary [14].

A more general open problem in secret sharing is the determination, for every access structure Γ, of the *optimal information rate* $\rho(\Gamma)$, that is, the information rate of the best secret sharing scheme for Γ. The *independent sequence method* is a general method to obtain upper bounds on the optimal information rate of an access structure [2, 10]. We describe in the following this method. For a clutter Λ on a set P, the *closure* $\mathrm{cl}(\Lambda)$ of Λ is formed by all subsets of P containing some subset in Λ. Obviously, $\mathrm{cl}(\Lambda)$ is monotone increasing. An *independent sequence* of *length* m and *size* s in the clutter Λ is a sequence $(B_1, \ldots, B_m \mid X_1, \ldots, X_m)$ of subsets of P satisfying:

1. $B_1 \subseteq \cdots \subseteq B_m \subseteq P$ and $s = |X_1 \cup \cdots \cup X_m|$, and
2. $B_i \cup X_i \in \mathrm{cl}(\Lambda)$ for $i = 1, \ldots, m$, and
3. $B_i \cup X_{i+1} \notin \mathrm{cl}(\Lambda)$ for $i = 1, \ldots, m-1$ and $B_m \notin \mathrm{cl}(\Lambda)$.

Independent sequences provide upper bounds on the optimal information rate of an access structure Γ. Specifically, if there exists in $\Lambda = \min \Gamma$ an independent sequence of length m and size s, then $\rho(\Gamma) \leq s/m$ [2, 10].

By combining the independent sequence method with the forbidden minor characterization of matroid ports by Seymour [11], a new characterization of matroid ports in terms of independent sequences has been obtained in a recent work [8].

Theorem 3. *A clutter is a matroid port if and only if it does not admit any independent sequence with length $m = 3$ and size $s = 2$, and in this case there does not exist in the clutter any independent sequence whose length m is greater than its size s.*

As a consequence of this new characterization of matroid ports, the result by Brickell and Davenport [4] on ideal access structures was generalized in [8].

Theorem 4. *If the optimal information rate of an access structure is greater than $2/3$, then its minimal qualified sets form a matroid port.*

Because of the applications to secret sharing, it would be interesting to have an efficiently checkable characterization of matroid ports. The algorithms to decide wether a given clutter is a matroid port or not that can be obtained from the existing characterizations are not efficient. Even though our main result (Theorem 1) is not a characterization, it provides a necessary condition for a clutter to be a matroid port that can be efficiently checked.

3 The Diameter of Matroid Ports

We present in this section the proof of our main result, Theorem 1. We begin by presenting three technical lemmas that are needed in the proof. The first one, Lemma 5, is due to Withney [16] and its proof can be derived from the one of [9, Proposition 4.1.2], while Lemma 6 was given in [11, Lemma 4]. By combining these two results we obtain Lemma 7, which will be used several times in the proof of Theorem 1.

Lemma 5. *Let C_1 and C_2 be two different circuits of a matroid $\mathcal{M}$ with $C_1 \cap C_2 \neq \emptyset$. Then, for every pair of points $c_1 \in C_1 - C_2$ and $c_2 \in C_2 - C_1$, there exists a circuit C of $\mathcal{M}$ such that $c_1, c_2 \in C \subseteq C_1 \cup C_2$.*

Lemma 6. *Let Λ be a matroid port and let $A \in \Lambda$ and $C \in \mathcal{C}_2(\Lambda)$ with $A \cap C \neq \emptyset$. Then there exist distinct subsets $A_1, A_2 \in \Lambda$ such that $A_1, A_2 \subseteq A \cup C$ and $C = E(A_1 \cup A_2)$.*

Lemma 7. *Let Λ be a connected matroid port on a set P, and let $p_1, p_2 \in P$ be two points such that there does not exist any set $A \in \Lambda$ with $\{p_1, p_2\} \subseteq A$. Then, for every pair of subsets $A_1, A_2 \in \Lambda$ with $p_1 \in A_1$ and $p_2 \in A_2$, there exist $A'_1, A'_2 \in \Lambda(A_1 \cup A_2)$ such that $\Lambda(A'_1 \cup A'_2) = \{A'_1, A'_2\}$, and $p_1 \in A'_1$ and $p_2 \in A'_2$.*

Proof. Let $\mathcal{M}$ be the matroid with ground set $Q = P \cup \{p_0\}$ such that $\Lambda = \mathcal{M}_{p_0}$ and consider the circuits $C_i = A_i \cup \{p_0\}$ for $i = 1, 2$. From Lemma 5, there exists a circuit C of $\mathcal{M}$ such that $p_1, p_2 \in C \subseteq C_1 \cup C_2 = A_1 \cup A_2 \cup \{p_0\}$. Observe that $C \notin \mathcal{C}_1(\Lambda)$ because there does not exist $A \in \Lambda$ with $p_1, p_2 \in A$. By applying Lemma 6 to $A_1 \in \Lambda$ and $C \in \mathcal{C}_2(\Lambda)$ (notice that $p_1 \in A_1 \cap C \neq \emptyset$), there exist $A'_1, A'_2 \in \Lambda$ with $A'_1, A'_2 \subseteq A_1 \cup C$ such that $C = E(A'_1 \cup A'_2)$. Since $A_1 \cup C \subseteq A_1 \cup C_1 \cup C_2 = A_1 \cup A_2 \cup \{p_0\}$, we get that $A'_1, A'_2 \in \Lambda(A_1 \cup A_2)$. In addition, since $p_1, p_2 \in C = E(A'_1 \cup A'_2) \subseteq A'_1 \cup A'_2$, we may assume without loss of generality that $p_1 \in A'_1$ and $p_2 \in A'_2$. The proof is concluded by checking that $\Lambda(A'_1 \cup A'_2) = \{A'_1, A'_2\}$. Assume that there exists $A \in \Lambda(A'_1 \cup A'_2) - \{A'_1, A'_2\}$. Then $A'_i \cup A \subseteq A'_1 \cup A'_2$ for $i = 1, 2$, which implies that $E(A'_i \cup A) \subseteq E(A'_1 \cup A'_2)$. Since the circuit $C = E(A'_1 \cup A'_2)$ is a minimal element in $\mathcal{C}_2^+(\Lambda)$, we get that $E(A'_i \cup A) = E(A'_1 \cup A'_2)$ for $i = 1, 2$. Therefore, $p_1 \in A$ because $p_1 \in C = E(A'_1 \cup A'_2) = E(A'_2 \cup A) \subseteq A'_2 \cup A$ and $p_1 \notin A'_2$. Symmetrically, $p_2 \in A$. This is a contradiction because we are assuming that $\{p_1, p_2\} \nsubseteq A$ for every $A \in \Lambda$. □

We can proceed now with the proof of Theorem 1. Assume that the result is false and consider a path-connected matroid port Λ on a set P with diameter at least 3. In such a case there exist two different points $p_1, p_2 \in P$ such that $d_\Lambda(p_1, p_2) = 3$. Now, among the paths of length three from p_1 to p_2, consider a path $\Pi_0 = (A_1, A_2, A_3)$ such that the number of points in $A_1 \cup A_2 \cup A_3$ is minimum. Clearly, $p_1 \in A_1 - (A_2 \cup A_3)$ and $p_2 \in A_3 - (A_1 \cup A_2)$. Moreover, $A_1 \cap A_3 = \emptyset$ while both $A_1 \cap A_2$ and $A_2 \cap A_3$ are nonempty. Consider two points $q_1 \in A_1 \cap A_2$ and $q_2 \in A_2 \cap A_3$.

In the following, we prove several properties of the induced clutters $\Lambda(A_1 \cup A_3)$, $\Lambda(A_1 \cup A_2)$, $\Lambda(A_2 \cup A_3)$, and $\Lambda(A_1 \cup A_2 \cup A_3)$.

Claim 8. $\Lambda(A_1 \cup A_3) = \{A_1, A_3\}$.

Proof. By Lemma 7, there exist $A'_1, A'_3 \in \Lambda(A_1 \cup A_3)$ with $p_1 \in A'_1$ and $p_2 \in A'_3$ such that $\Lambda(A'_1 \cup A'_3) = \{A'_1, A'_3\}$. Observe that $A'_1 \cap A_3 = \emptyset$ and $A_1 \cap A'_3 = \emptyset$ because $d_\Lambda(p_1, p_2) > 2$. Since $A'_1 \cup A'_3 \subseteq A_1 \cup A_3$, we get that $A'_i \subseteq A_i$ for $i = 1, 3$, and hence $A'_i = A_i$ because Λ is a clutter. □

Claim 9. *For $i = 1, 3$, there exists $D_i \in \Lambda(A_i \cup A_2)$ such that $\Lambda(A_i \cup D_i) = \{A_i, D_i\}$, such that $A_1 \cup D_i \cup A_3 = A_1 \cup A_2 \cup A_3$, and $\Pi_i = (A_1, D_i, A_3)$ is a path from p_1 to p_2.*

Proof. By symmetry, it is enough to prove the existence of D_1. From Lemma 7 applied to the sets $A_1, A_2 \in \Lambda$ and to the points $p_1 \in A_1$ and $q_2 \in A_2$, there exist $A'_1, A'_2 \in \Lambda(A_1 \cup A_2)$ such that $p_1 \in A'_1$, and $q_2 \in A'_2$, and $\Lambda(A'_1 \cup A'_2) = \{A'_1, A'_2\}$.

We prove in the following that $A'_1 \cap A'_2 \neq \emptyset$. This is clear if $A'_1 = A_1$ or $A'_2 = A_2$. Suppose that $A'_1 \neq A_1$ and $A'_2 \neq A_2$. Then $A'_1 \cap A_2 \neq \emptyset$ and $\Pi' = (A'_1, A_2, A_3)$ is a path of length three from p_1 to p_2. Since $\Pi_0 = (A_1, A_2, A_3)$ is a path with a minimum number of points, $|A_1 \cup A_2 \cup A_3| \leq |A'_1 \cup A_2 \cup A_3|$, and hence $A_1 \cup A_2 \cup A_3 = A'_1 \cup A_2 \cup A_3$ and $A_1 - A_2 \subseteq A'_1$. In addition, $A'_2 \cap (A_1 - A_2) \neq \emptyset$ because $A'_2 \subseteq A_1 \cup A_2$ and $A'_2 \neq A_2$. This implies that $A'_1 \cap A'_2 \neq \emptyset$.

Therefore, $\Pi'_1 = (A'_1, A'_2, A_3)$ is a path of length three from p_1 to p_2. By taking into account the minimality on the number of points involved in the path Π_0, we conclude that $A_1 \cup A_2 \cup A_3 = A'_1 \cup A'_2 \cup A_3$. Since $A_1 \subseteq A'_1 \cup A'_2$ and $\Lambda(A'_1 \cup A'_2) = \{A'_1, A'_2\}$, we get that $A_1 = A'_1$. The proof is concluded by taking $D_1 = A'_2$. □

Claim 10. *There exists $A \in \Lambda - \{A_1, A_2, A_3\}$ with $A \subseteq A_1 \cup A_2 \cup A_3$.*

Proof. Assume that the claim is false. Consider the subsets $B_1 = (A_1 \cup A_2 \cup A_3) - \{p_1, p_2, q_1, q_2\}$, and $B_2 = B_1 \cup \{p_1\}$, and $B_3 = B_1 \cup \{p_1, p_2\}$, and also the subsets $X_1 = \{q_1, q_2\}$, and $X_2 = \{q_1\}$, and $X_3 = \{q_2\}$. On one hand we have that $A_2 \subseteq B_1 \cup X_1$, and $A_1 \subseteq B_2 \cup X_2$, and $A_3 \subseteq B_3 \cup X_3$. Therefore the three subsets $B_1 \cup X_1$, $B_2 \cup X_2$, and $B_3 \cup X_3$ are in $\mathrm{cl}(\Lambda)$. On the other hand, since $p_1 \in A_1$, $p_2 \in A_3$, and $q_1, q_2 \in A_2$, it follows that the subsets $B_1 \cup X_2$, $B_2 \cup X_1$, and B_3 are not in $\mathrm{cl}(\Lambda)$. Therefore $(B_1, B_2, B_3 \,|\, X_1, X_2, X_3)$ is an independent sequence with length $m = 3$ and size $s = 2$, a contradiction by Theorem 3. □

Claim 11. *If $A \in \Lambda(A_1 \cup A_2 \cup A_3) - \{A_1, A_2, A_3\}$, then $p_1, p_2 \notin A$ and $A_1 \cup A_2 \cup A_3 = A_1 \cup A \cup A_3$.*

Proof. Consider $A \in \Lambda - \{A_1, A_2, A_3\}$ with $A \subseteq A_1 \cup A_2 \cup A_3$. We prove first that both $A \cap A_1$ and $A \cap A_3$ are nonempty by using the sets D_1, D_3 introduced in Claim 9. Suppose that $A \cap A_1 = \emptyset$. Since $A \subseteq A_1 \cup A_2 \cup A_3 = A_1 \cup D_3 \cup A_3$, we get that $A \subseteq D_3 \cup A_3$. This, combined with $\Lambda(D_3 \cup A_3) = \{D_3, A_3\}$, implies that $A = D_3$, a contradiction because $A_1 \cap D_3 \neq \emptyset$ by Claim 9. Symmetrically, $A \cap A_3 \neq \emptyset$. Therefore $p_1, p_2 \notin A$ because $d_\Lambda(p_1, p_2) = 3$. In addition, $\Pi = (A_1, A, A_3)$ is a path of length three from p_1 to p_2, which implies that $A_1 \cup A_2 \cup A_3 = A_1 \cup A \cup A_3$ by the minimality of the path Π_0. □

At this point, we conclude the proof of Theorem 1 by showing an independent sequence that leads to contradiction. From Claim 8, we have $A_2 \nsubseteq A_1 \cup A_3$, while it follows from Claim 10 that there exists a set $A_4 \in \Lambda(A_1 \cup A_2 \cup A_3) - \{A_1, A_2, A_3\}$. Therefore we can take a point $q_3 \in A_2 - (A_1 \cup A_3)$ and a point $q_4 \in A_4 - A_2$. Because of the symmetry between A_1 and A_3, we can suppose without loss of generality that $q_4 \in A_1$. Consider the subsets $B_1 = A_4 - \{q_3, q_4\}$, $B_2 = (A_2 \cup A_4) - \{q_3, q_4\}$, and $B_3 = (A_1 \cup A_2 \cup A_4) - \{q_3, q_4\}$. Consider as well the subsets $X_1 = \{q_3, q_4\}$, $X_2 = \{q_3\}$, and $X_3 = \{q_4\}$. Clearly $A_4 = B_1 \cup X_1$, and $A_2 \subseteq B_2 \cup X_2$, and $A_1 \subseteq B_3 \cup X_3$, which implies that $B_i \cup X_i \in \mathrm{cl}(\Lambda)$ for $i = 1, 2, 3$. Obviously, $B_1 \cup X_2 = A_4 - \{q_4\} \notin \mathrm{cl}(\Lambda)$. In addition, $A_i \nsubseteq B_2 \cup X_3$ and $A_i \nsubseteq B_3$ for $i = 1, 2, 3$. Moreover, from Claim 11, if $A \in \Lambda(A_1 \cup A_2 \cup A_3) - \{A_1, A_2, A_3\}$, then

$q_3 \in A$, and hence $A \nsubseteq B_2 \cup X_3$ and $A \nsubseteq B_3$. Therefore $B_2 \cup X_3, B_3 \notin \mathrm{cl}(\Lambda)$ and $(B_1, B_2, B_3 \,|\, X_1, X_2, X_3)$ is an independent sequence with length $m = 3$ and size $s = 2$, which is a contradiction by Theorem 3. This concludes the proof of Theorem 1.

4 Related Results and Applications to Secret Sharing

The converse of Theorem 1 does not hold. On the set $P = \{p_1, p_2, p_3, p_4\}$, consider the clutters $\Lambda_1 = \{\{p_1, p_2\}, \{p_1, p_3\}, \{p_1, p_4\}, \{p_2, p_3, p_4\}\}$ and $\Lambda_2 = \{\{p_1, p_2\}, \{p_1, p_3\}, \{p_2, p_3, p_4\}\}$. The diameters of Λ_1 and Λ_2 are equal to 1 and 2, respectively. As a consequence of Seymour's characterization [11], none of these clutters is a matroid port. This fact can be easily proved from Theorem 3 as well.

Therefore, we cannot obtain a characterization of matroid ports from our main result. Nevertheless, it provides an efficiently checkable necessary condition for a clutter to be a matroid port. Because of the connections between matroid ports and the access structures of ideal secret sharing schemes that were described in Section 2, our result can be applied to secret sharing. The next corollary is a direct consequence of Theorems 1 and 4.

Corollary 12. *Let Γ be an access structure such that the clutter $\min \Gamma$ is path-connected. Then $\rho(\Gamma) \leq 2/3$ if the diameter of $\min \Gamma$ is greater than 2.*

Therefore, given an access structure Γ such that the clutter $\min \Gamma$ is path-connected, we compute the diameter of $\min \Gamma$. If this diameter is greater than 2, we conclude that $\min \Gamma$ is not a matroid port, and hence there is no ideal secret sharing scheme for Γ and, moreover, its optimal information rate is $\rho(\Gamma) \leq 2/3$. Nevertheless, we cannot say much about the optimal information of Γ if the diameter of $\min \Gamma$ is 1 or 2.

There is no other restriction on the values of the diameters of matroid ports than the one in Theorem 1. Consider two integers k, n with $1 \leq k \leq n$. The ground set of the *uniform matroid* $U_{k,n}$ has n points, while its circuits are all subsets with exactly $k+1$ points. If $2 \leq k < n$, the diameter of every port of the uniform matroid $U_{k,n}$ is equal to 1. Consider a connected matroid $\mathcal{M} = (Q, \mathcal{C})$ and a point $p_0 \in Q$ such that the matroid port $\mathcal{M}_{p_0}$ is path-connected and there exist two different points $\{p_1, p_2\} \in Q - \{p_0\}$ such that $\{p_1, p_2\}$ is a circuit of $\mathcal{M}$. Then the diameter of the matroid port $\mathcal{M}_{p_0}$ is equal to 2 because $d_{\mathcal{M}_{p_0}}(p_1, p_2) = 2$. An example of such a matroid is the one with ground set $Q = \{p_0, p_1, p_2, p_3\}$ and circuits $\mathcal{C} = \{\{p_1, p_2\}, \{p_0, p_1, p_3\}, \{p_0, p_2, p_3\}\}$.

Even though it is not possible to improve Theorem 1, next we prove a property of matroid ports with diameter equal to two which involves its *dual*. The *dual* Λ^* of a clutter Λ on a set P is defined as the collection of the minimal sets that have nonempty intersection with all members of Λ, that is

$$\Lambda^* = \min\{B \subseteq P \,:\, B \cap A \neq \emptyset \text{ for all } A \in \Lambda\}.$$

The dual of a clutter is also is a clutter, and $\Lambda^{**} = \Lambda$. Now, given two points in P, we can consider the distance between these points both in the clutter Λ and in its dual Λ^*. The next proposition establish the relationship between both distances whenever Λ is a matroid port.

Proposition 13. *Let Λ be a matroid port on a set of points P, and let $p_1, p_2 \in P$ be two points such that $d_\Lambda(p_1, p_2) = 2$. Then, $d_{\Lambda^*}(p_1, p_2) = 1$.*

Proof. Since $d_\Lambda(p_1, p_2) = 2$, then by Lemma 7 there exist $A'_1, A'_2 \in \Lambda(A_1 \cup A_2)$ with $p_1 \in A'_1$ and $p_2 \in A'_2$ such that $\Lambda(A'_1 \cup A'_2) = \{A'_1, A'_2\}$. Observe that

$$\Lambda = \Lambda^{**} = \min\{C \subseteq P \,:\, C \cap B \neq \emptyset \text{ for all } B \in \Lambda^*\}.$$

Since $A \nsubseteq (A'_1 \cup A'_2) - \{p_1, p_2\}$ for every $A \in \Lambda$, there must exist a subset $B \in \Lambda^*$ such that $B \cap ((A'_1 \cup A'_2) - \{p_1, p_2\}) = \emptyset$. In addition, $A'_i \cap B \neq \emptyset$ for $i = 1, 2$ because $A'_i \in \Lambda$ and $B \in \Lambda^*$. Therefore $p_1, p_2 \in B$, and hence $d_{\Lambda^*}(p_1, p_2) = 1$. □

Proposition 13 has also an interesting application to secret sharing that is related to the construction of *multiplicative linear secret sharing schemes*. All definitions and basic results on this topic can be found in [5]. The *dual* of an access structure Γ is the access structure $\mathrm{cl}((\min \Gamma)^*)$. Let Γ be the access structure of an ideal linear secret sharing scheme. Then $\min \Gamma$ is a matroid port. Suppose that there exist two participants at distance 2 in the clutter $\min \Gamma$. then it is clear from Proposition 13 that $\Gamma^* \nsubseteq \Gamma$. This means that the access structure Γ is not $\mathcal{Q}_2$, and hence that Γ does not admit a multiplicative linear secret sharing scheme.

References

[1] G.R. Blakley. Safeguarding cryptographic keys. *AFIPS Conference Proceedings* **48** (1979) 313–317.

[2] C. Blundo, A. De Santis, R. De Simone, U. Vaccaro. Tight bounds on the information rate of secret sharing schemes. *Des. Codes Cryptogr.* **11** (1997) 107–122.

[3] E.F. Brickell. Some ideal secret sharing schemes. *J. Combin. Math. Combin. Comput.* **9** (1989) 105–113.

[4] E.F. Brickell, D.M. Davenport. On the classification of ideal secret sharing schemes. *J. Cryptology* **4** (1991) 123–134.

[5] R. Cramer, V. Daza, I. Gracia, J. Jiménez Urroz, G. Leander, J. Martí-Farré, C. Padró. On codes, matroids and secure multi-party computation from linear secret sharing schemes. *Advances in Cryptology - CRYPTO 2005, Lecture Notes in Comput. Sci.* **3621** (2005) 327–343.

[6] A. Lehman. A solution of the Shannon switching game. *J. Soc. Indust. Appl. Math.* **12** (1964) 687–725.

[7] A. Lehman. Matroids and Ports. *Notices Amer. Math. Soc.* **12** (1965) 342–343.

[8] J. Martí-Farré, C. Padró. On Secret Sharing Schemes, Matroids and Polymatroids. *Fourth IACR Theory of Cryptography Conference TCC 2007, Lecture Notes in Comput. Sci.* **4392** (2007) 273–290.

[9] J. G. Oxley. *Matroid Theory.* Oxford University Press, 1992.

[10] C. Padró, G. Sáez. Secret sharing schemes with bipartite access structure. *IEEE Trans. Inform. Theory* **46** (2000) 2596–2604.

[11] P. D. Seymour. A forbidden minor characterization of matroid ports. *Quart. J. Math. Oxford Ser.* **27** (1976) 407–413.

[12] P. D. Seymour. On secret sharing matroids. *J. Combin. Theory Ser. B* **56** (1992) 69–73.

[13] A. Shamir. How to share a secret. *Comm. ACM* **22** (1979) 612–613.

[14] J. Simonis, A. Ashikhmin. Almost affine codes. *Des. Codes Cryptogr.* **14**(2) (1998) 179–197.

[15] D. R. Stinson. An explication of secret sharing schemes. *Des. Codes Cryptogr.* **2** (1992) 357–390.

[16] H. Whitney. On the abstract properties of linear dependence. *Amer. J. Math.* **57** (1935) 509–533.